Biometrics verification in a real environment

Belén Ruiz-Mezcua (*), Dolores Garcia-Plaza (**), Cristina Fernandez (**),
Paloma Domingo-García (*) and Fernando Fernandez (**)
(*): Universidad Carlos III de Madrid
email:Bruiz@inf.uc3m.es
c/ Butarque, 15
28911 Leganés (Madrid). Spain
Tel: 34-1-6249417 Fax:34-1-6249430
(**): Ibermatica-Madrid
Avda. Partenón 16-18. Madrid. Spain
Tel: 34 - 913849100 Fax: 34 - 913849144

Abstract

This paper describes some of the biometrics verification applications developed within the project ACTS-102 M2VTS: Multimodal Verification for Teleservices and Security Applications. These prototypes provide identity authentication in two of the most promising application areas of biometrics: Secured access to financial services (ATM and Internet Teleservices) and building security applications.

The verification modalities implemented into the prototypes are face and speech verification, these are potentially the best accepted by users since they are the less intrusive and the more inexpensive. To achieve higher levels of security, the results obtained by each modality are combined using a fusion method, which decides the user acceptance or rejection.

Every prototype has been tested by end-users in a close to real environment.

Keyword List : Applications, multimodal biometrics verification, teleservices security.

INTRODUCTION

This paper shows three different applications in user verification using two biometric technologies: Face image verification and speaker verification.

The first prototype, called UTAP1, provides secure access to the R&D department of the UTAP (Technical Assistant Unit of the Basque Country Police).

The second one, BBV1, controls the access to the ATMs of the Banco Bilbao Vizcaya, while the last of these applications provides access control to telebanking services through Internet. The prototypes use standard hardware, PC based computers and commercial acquisition devices. The biometrics technology has been developed within the M2VTS project. This design allows easily maturing the prototypes to low cost products available to a wide market.

BBV1 SYSTEM: TELESERVICES APPLICATIONS: CASH DISPENSERS

The objective of this application is to control and to verify the identity of the persons that wish to accede to different teleservices provided by the Banco Bilbao Vizcaya through its ATM net. The system is composed of a camera, that takes the frontal image of the face of the user and of a microphone that permit the use of the voice, in addition to a badge reader.

Application Scenario

Users identification is carried out by means of their identity badge. The verification is done through the frontal image of the faces of individuals trying to accede to the system and through the monitoring of their voices. In the case of multiple rejections, users are allowed to use other traditional monitoring methods such as personal identification code, etc.

The verification and fusion algorithms integrated have been developed by several partners of the M2VTS consortium. Face verification is based on MDLA (Morphological Dynamic Link Architecture) while speaker authentication is based on Gaussian Mixed Model (GMM) [5][6] and has been developed by CIII. The size of the images captured is 320x240 greyscale for face image algorithms.

0-7803-5247-5/99/$10.00 ©1999 IEEE

The voice has been recorded at 8 kHz. 16 bits per sample. In each session the user speaks between 20 and 30 seconds.

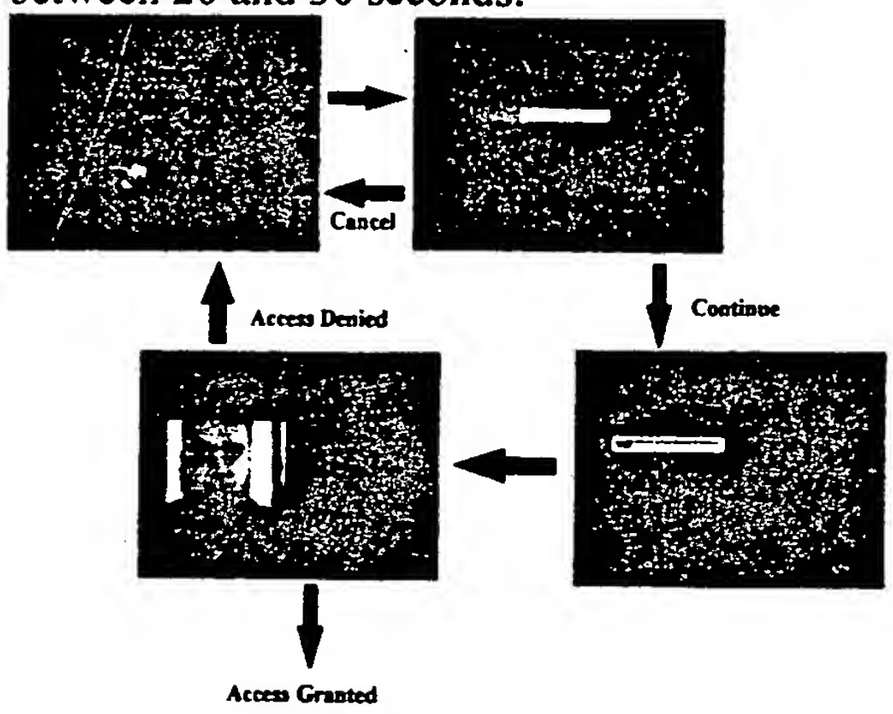

Figure 1: Screen sequence

Hardware Architecture

The system is composed of one or more operator consoles, implemented in Pentium PC running Windows NT or 95. The training step or user enrolment is performed in these consoles. The user authentication and access to the bank services is performed in ATMs. The ATM will be based in a Pentium PC equipped with camera and microphone. The recording systems are conveniently hidden and protected against vandalism and weather conditions.

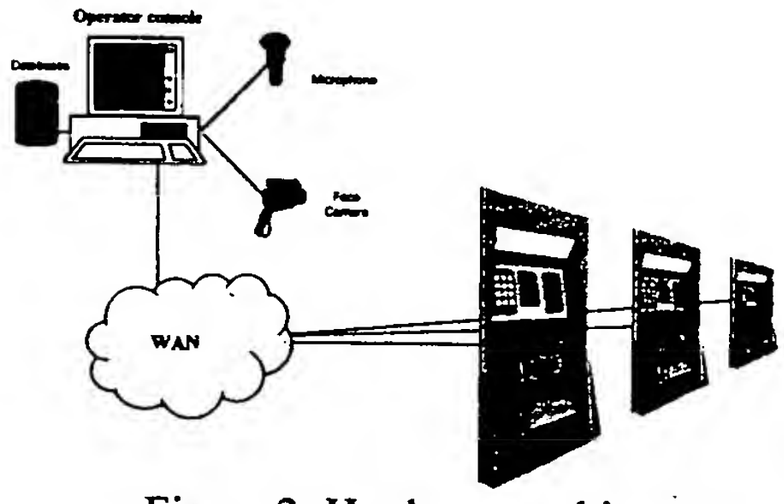

Figure 2: Hardware architecture

Field Test

The application field tests were designed to achieve two main objectives. On one hand to test the biometric authentication technology developed in the project in a real environment. On the other hand, to obtain information from the end-users about the usability of the prototypes and future improvements.

User Typology

The training and verification test sets are both composed of 17 people from the Ibermatica R&D department staff and BBV staff.

- Sex distribution: 12 male and 5 female.
- Ages: Ranging from 22 to 35

Environment description

The environment was prepared trying to imitate the conditions in a real ATM. The equipment was installed in a corner between two windows in order to get the outdoor lighting conditions. The noise level was also rather high.

Results obtained and Statistical Description

The test performed in Ibermatica could be summarised in the following figures:

Total number of impostor claims:	6460
Total number of client claims:	340

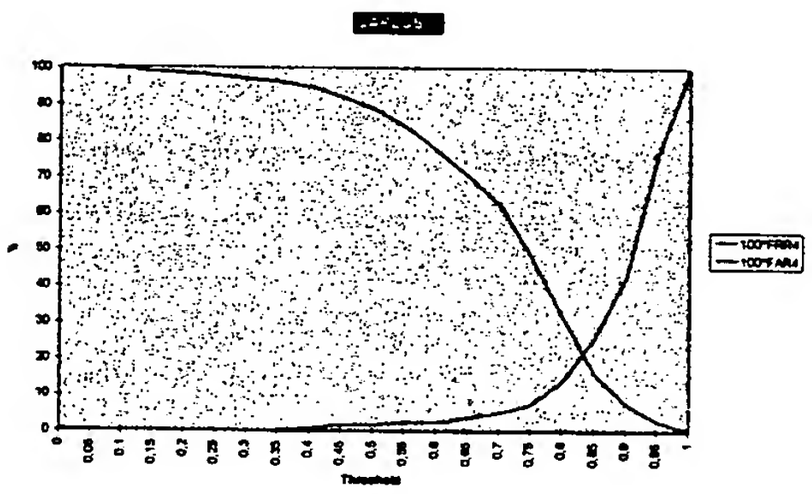

Figure 3: ROC curves to speech verification

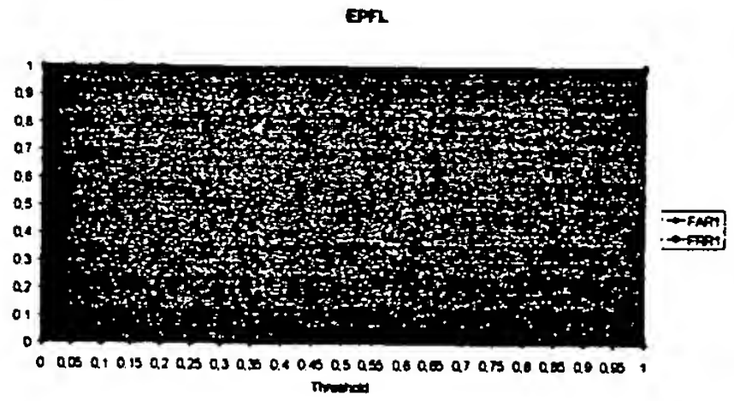

Figure 4: ROC curves to image verification

The multimedia verification after fusion procedure could be shows in the following picture

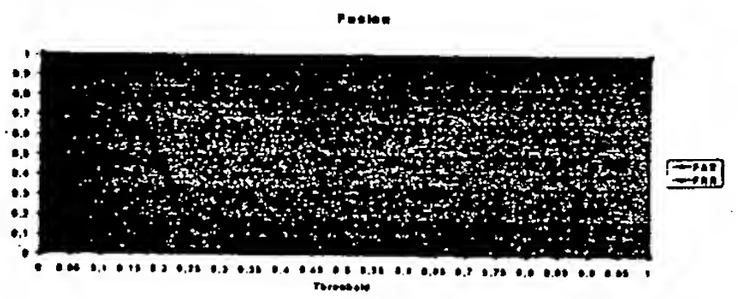

Figure 5: ROC curves to user verification

Teleservices Applications through INTERNET

The objective of this application is to provide secure access to teleservices, specially banking teleservices, through Internet. The user that

accedes to this kind of services must authenticate their identity by means of his voice and face image.
The cost of the system cannot be very expensive since it must be accessible to a wide range of user. Therefore standard technology has been selected such as low cost videoconference cameras and Sound Blaster audio digitizer. The navigator selected is Microsoft Explorer and the Web server is Internet Information Server.

Application Scenario

The identification of the user is done by a code given by an administrator, the verification is done by frontal view face image and voice. Operation mode is similar to the biometric ATM described above, but in this case the verification process is done though the Internet navigator.

Figure 6: Face image acquisition page

Hardware Architecture

The Web server is a Pentium PC that provides the services of HTML, ASP and FTP. The Web clients are also Pentium PC equipped with low cost digital cameras, Sound Blaster or compatible cards and microphone.

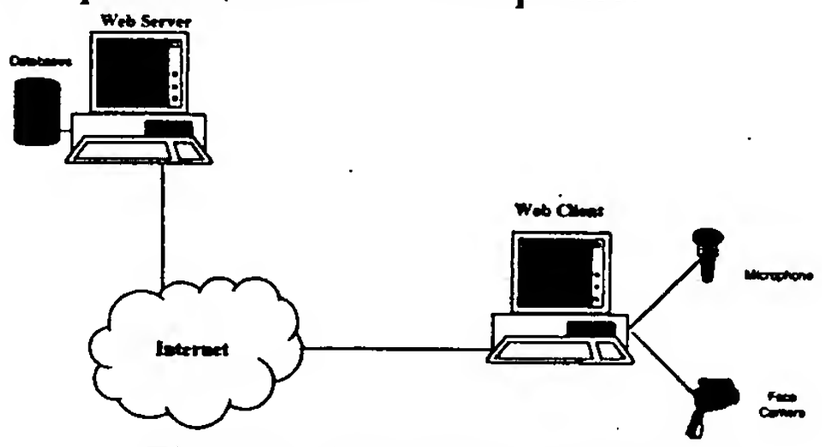

Figure 7: Hardware architecture

Field tests

The application has been tested in an office environment using natural light. The background for frontal images is not uniform, being the background.

The training and verification test sets are both composed of 17 people from Ibermatica and BBV staff.

- Sex distribution: 12 male and 5 female.
- Ages: Ranging from 22 to 35

All the impostor claims were done trying to impost the most similar person.

Total number of impostor claims:	131
Total number of client claims:	29

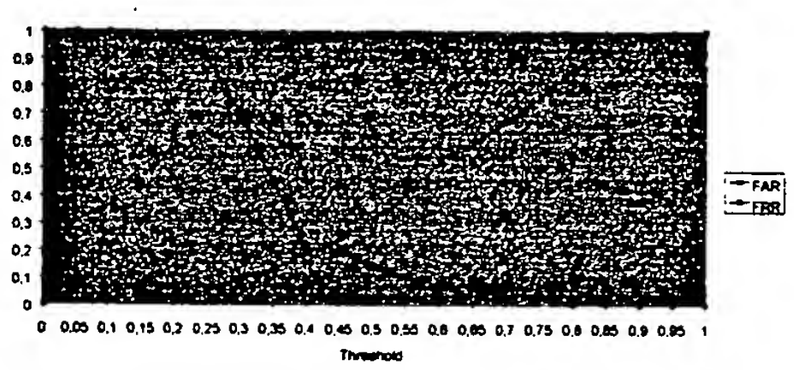

Figure 6 ROC curves to user verification

UTAP1: ACCESS CONTROL TO AN OFFICE DEPARTMENT

This application controls the only entrance to the R&D department of UTAP. The system is composed of two cameras installed in the wall and that will capture the front and profile images, and of a microphone or recording system of audio that permits the use of the voice.
The users identify through keyboard by typing the four digits of his code. Then, he speaks free text for a minimum of 15 seconds and a maximum of 30 seconds. Once his voice is verified his frontal image is captured. When the frontal image is verified the profile image is captured following the same procedure.
No operator station is considered when the system is operative, as the number of employees is not so big. Anyway, during the training there must be an operator.

Hardware Architecture

The system consists in a Pentium PC that acts as operator station and verification. It is equipped with a Meteor frame grabber and a Sound Blaster card. There are two video cameras connected one for the frontal view of the face and the other for the profile.

Headphones have been used as audio recording system.
In this case, there is an only access to control, but this architecture is completely scalable allowing adding as many stations as necessary. All the stations would be connected through an Ethernet LAN being one of them the disk server.

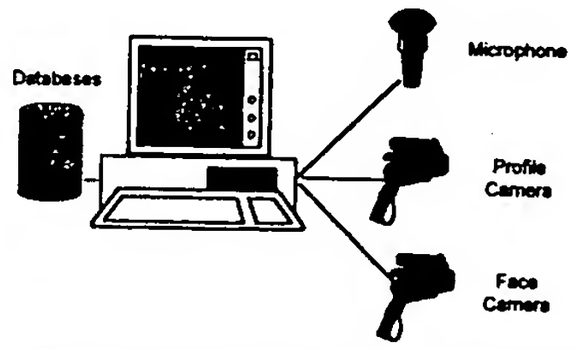

Figure 7: Data acquisition to UTAP prototype

Application Scenario
The UTAP1 application is composed of two separate programs, one for training and databases managing and one for operation. The size of the images captured is 320x240 greyscale for both image algorithms.
The scores provided by the algorithms are normalised between 0 and 1 following an only criterion for all the users. The fusion of the modality results is obtained by computing the weighted average of the scores. If the resulting number is greater than a global threshold the access is granted.

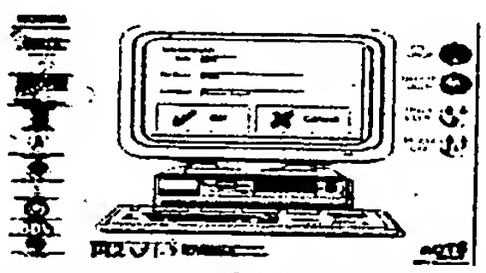

Figure 8: Appearance of UTAP Prototype

Field tests
This prototype has been tested by 4 people all of them members of the R&D department of UTAP. The database for training is composed of 20 people.

- Sex distribution: 2 male and 2 female.
- Ages: Ranging from 27 to 38.

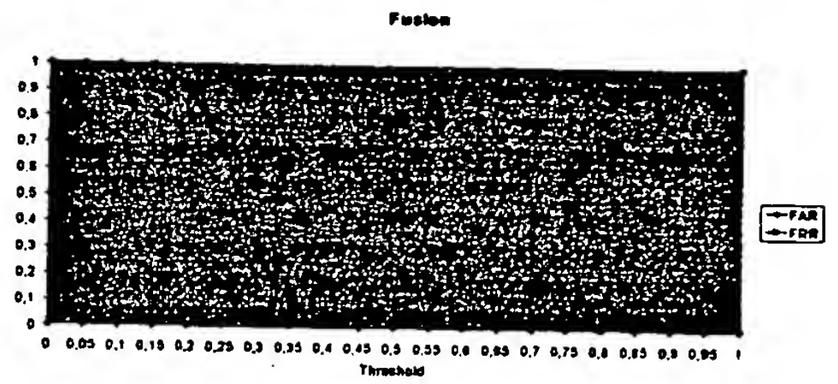

Figure9: ROC curves to user verification

CONCLUSIONS

There is now a potential but immense market to biometric applications, which demands new and more efficient authentication methods to protect data in the new working environments.
The results achieved in the M2VTS project as well as the excellent comments of European Commission reviewers' about the project motivate us to follow working in this area. Future work will be devoted to develop more usable interfaces to biometric technology as well as to improve the robustness of verification algorithms in variable environment conditions. The objective will be to evolve the current prototypes into products, which satisfy the common user requirements.

REFERENCES

[1] M2VTS Consortium. Multi Modal Verification for Teleservices and Security Applications. IEEE Multimedia Systems. ICMS99.
[2] C. Kotropoulos, A. Tefas, I. Pitas, C. Fernandez, F. Fernandez. Performance Assessment Of Morphological Dynamic Link Architecture Under Optimal And Real Operating Conditions. NSIP99. Antalya, Turkey
[5] B. Ruiz, P. Domingo, L. Hernandez. A Dual Speech/Speaker Recognition Using GMM In Speaker Identification And A HMM In Keyword Speech Recognition. ICCST99. Madrid, Spain.
[6] E. Rodriguez, B. Ruiz, A. Garcia_Crespo. Speech/Speaker Recognition using a HMM/GMM Hybrid model. AVBPA 97.